



## **SARGOS : Système d'Alerte et Réponse Graduée Off Shore**

Marie-Annick Giraud, André van Graver, Aldo Napoli, Christian Scapel,  
Denis Chaumartin, Michel Morel, Eric Itcia, David Bonacci

### **► To cite this version:**

Marie-Annick Giraud, André van Graver, Aldo Napoli, Christian Scapel, Denis Chaumartin, et al.. SARGOS : Système d'Alerte et Réponse Graduée Off Shore. Conférence WISG - Workshop Interdisciplinaire sur la Sécurité Globale, Jan 2010, Troyes, France. 8 p. hal-00751293

**HAL Id: hal-00751293**

**<https://hal-mines-paristech.archives-ouvertes.fr/hal-00751293>**

Submitted on 18 Jan 2013

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# « SARGOS »

## Système d'Alerte et Réponse Graduée Off Shore

Marie-Annick GIRAUD<sup>1</sup>, André VAN GAVER<sup>1</sup>, Aldo NAPOLI<sup>2</sup>, Christian SCAPEL<sup>3</sup>, Denis CHAUMARTIN<sup>4</sup>, Michel MOREL<sup>5</sup>, Eric ITCIA<sup>6</sup>, David BONACCI<sup>7</sup>

<sup>1</sup> SOFRESUD, 777 av. de Bruxelles, 83500 La Seyne sur Mer

<sup>2</sup> ARMINES/CRC, Rue Claude Daunesse, 06904 Sophia Antipolis

<sup>3</sup> CDMT, 3 avenue Robert Schuman, 13628 Aix en Provence Cedex 1

<sup>4</sup> CS Communication & Système, 230 Rue Marcellin Berthelot, 83130 La Garde

<sup>5</sup> DCNS Division Systèmes d'Information et de Sécurité, BP 403, 83055 Toulon Cedex

<sup>6</sup> ROCKWELL COLLINS France (RCF), 6 avenue Didier Daurat, BP 20008, 31701Blagnac Cedex

<sup>7</sup> TêSA, Télécommunications Spatiales et Aéronautiques, 14-16 Port Saint Etienne, 31000 Toulouse.

[magiraud@sofresud.com](mailto:magiraud@sofresud.com) ; [avangaver@sofresud.com](mailto:avangaver@sofresud.com) ; [Aldo.Napoli@crc.ensmp.fr](mailto:Aldo.Napoli@crc.ensmp.fr) ; [denis.chaumartin@c-s.fr](mailto:denis.chaumartin@c-s.fr) ; [secretariat.cdmt@univ-cezanne.fr](mailto:secretariat.cdmt@univ-cezanne.fr) ; [michel.morel@dcnsgroup.com](mailto:michel.morel@dcnsgroup.com) ; [eitcia@rockwellcollins.com](mailto:eitcia@rockwellcollins.com) ; [david.bonacci@tesa.prd.fr](mailto:david.bonacci@tesa.prd.fr).

**Résumé** □ Le projet SARGOS propose de répondre au fort besoin émergeant de sécurisation des infrastructures offshore civiles vulnérables aux actions de malveillance, de piraterie ou de terrorisme menées à partir de la mer. L'objectif du projet est de développer un système global d'alerte et de réponse graduée, prenant en charge l'ensemble du processus de protection de l'infrastructure depuis la détection d'une menace potentielle jusqu'à la mise en œuvre de la réaction.

SARGOS apporte une réponse nouvelle et innovante dans ce domaine de la sécurité maritime pour lequel il n'existe pas aujourd'hui de système opérationnel. Un enjeu fort est mis sur la prise en compte des modes de fonctionnement de l'infrastructure et des contraintes réglementaires et juridiques. L'aspect novateur réside en premier lieu dans le caractère global de l'approche retenue, et ensuite dans son articulation dans les trois niveaux suivants :

- a) Le niveau d'une détection sûre d'un objet marin de faible dimension dans un périmètre de protection rapproché par mer agitée en utilisant des formes d'ondes radar continues innovantes couplées à de nouveaux algorithmes de traitement de signal ;
- b) Le niveau d'élaboration d'un plan de réaction vis-à-vis de l'intrusion décelée, prenant en compte l'enrichissement progressif de la connaissance et de la nature de l'objet détecté par des attributs de caractérisation de celui-ci. Le processus d'acquisition de la connaissance employé permet le déclenchement au moment approprié de réponses graduées prenant en compte le contexte de la crise (règles de sécurité en vigueur sur la plate-forme, environnement géopolitique, aspects juridiques) ;
- c) Le niveau de gestion de la panoplie des moyens de réaction, soit internes à la plate-forme offshore (mise en sécurité), soit externes pour riposter à la menace (injonction, intimidation, activation de moyens non létaux) et diffuser l'alerte vers les autorités locales.

**Abstract** □ The SARGOS Project aims to satisfy the strong emerging need to improve safety for the civilian offshore infrastructures, sensitive to the actions conducted by spite, piracy or terrorism on sea.

SARGOS brings a new and innovative answer in this field of maritime security. A special care is taken to comply with the infrastructures operational constraints and the contractual and legislative rules. The innovative part of the project is mainly the global approach used, based on three levels:

- a) The level of a safe detection of a small size marine object, in a small range protection area, with rough sea, using innovative CW radar waveforms improved by new efficient signal processing algorithms
- b) The level of construction of a response plan facing a detected intrusion, taking into account the progressive improvement of the knowledge and the kind of detected object defined by its characterisation attributes. The acquisition process allows appropriate responses taking into account the crisis situation. (Platform safety rules, geopolitical environment and legal aspects).
- c) The managing level of the variety of non-lethal response means, either internal to the offshore platform (safety mode), or external to reply to the menace (injunction, intimidation or activation of authorised means) and broadcast the alert to the local authorities.

## 1. Introduction

Les installations parapétrolières offshore sont des infrastructures énergétiques cruciales à l'échelle mondiale. A ce titre, elles constituent des cibles privilégiées pour des actions terroristes ou de piraterie en provenance de la mer.

Le renforcement de la sécurité maritime est devenu une priorité majeure des gouvernements après les événements de septembre 2001. Il s'est concrétisé notamment par la définition et la ratification du code international ISPS. Mais même dans ce contexte, la protection directe de chaque plate-forme à travers la mise en place de mesures de sécurité appropriées in situ relève toujours de la responsabilité industrielle.

Sur ces sites, le moyen de surveillance de base demeure le radar à impulsions de veille côtière ou de navigation, non adapté à la détection de la menace constituée par des esquifs ou des engins nautiques rapides et de faibles dimensions chargés d'explosifs (de type dinghy, vedette rapide ou « jet ski ») qui rechercheraient la collision ou l'abordage avec la plate-forme ou les navires en cours de chargement dans un terminal pétrolier ou gazier. En outre lors d'une intrusion avérée, il n'y a pas ou peu de règles formalisées pour réagir par des procédures de sauvegarde et par la mise en œuvre de moyens de dissuasion autonomes.

Il s'avère donc primordial d'augmenter le degré de protection de ces infrastructures en développant un nouveau système capable de générer une alarme et d'enclencher des réactions internes et externes en cas d'intrusion confirmée.

Le projet SARGOS répond à ce nouveau besoin de protection d'infrastructures civiles vulnérables aux actes de piraterie ou de terrorisme menées à partir de la mer.

L'objectif est de proposer un système global innovant permettant la surveillance et la protection d'infrastructures sensibles en mer, en prenant en charge toute la chaîne de traitement, depuis la détection de la menace jusqu'à la mise en œuvre des moyens de réaction adaptés au niveau de dangerosité de l'intrusion détectée.

## 2. Contexte et état de l'art

### 2.1 Contexte et enjeux économiques

*« La sécurité énergétique fait partie des challenges économiques et sécuritaires les plus sérieux, aussi bien aujourd'hui que dans le futur. La croissance des économies du monde et des sociétés va de pair avec l'importance de l'énergie et de pair avec les infrastructures qui produisent et fournissent cette énergie. Les infrastructures énergétiques critiques fournissent le carburant qui permet à l'économie globale d'avancer et à nos sociétés de fonctionner ».*

C'est en ces termes que s'est ouverte l'allocation de l'OSCE (Organization for Security and Cooperation in Europe) lors de la réunion du comité Economique de l'OTAN du 22 septembre 2008 à Bruxelles.

Face à la raréfaction de la ressource pesant sur les infrastructures énergétiques terrestres, les compagnies pétrolières avaient dans un premier temps effectué un repositionnement tactique sur des unités de production en offshore. Cependant l'hypothèse selon laquelle ces installations seraient protégées du fait même de leur éloignement ne tient plus. L'attaque en juin 2008 des infrastructures offshore de Shell à 120 km au large des côtes du Nigéria (champ pétrolifère « Bonga ») ou celle de la plateforme TOTAL du champ d'Amenam en mai 2009, démontrent que l'éloignement n'est plus un réel gage de sécurité.

Alors que les attaques de navires se multiplient (2008 et 2009 sont marqués par une augmentation sans précédent des détournements en mer), les exemples d'attaques d'infrastructures énergétiques offshore sont pour le moment moins fréquents et moins médiatisés. Ils n'en sont pas moins extrêmement inquiétants en ce sens qu'ils dévoilent une grande vulnérabilité :

- Avril 2004 : Attaques contre les terminaux offshore de Khor al-Amaya et Al-Basra en Irak. Fermeture des installations pour un coût estimé à 40 millions de dollars.
- Janvier 2006 : Des hommes armés utilisent des vedettes rapides pour envahir la plate-forme « Benisede » dans le détroit du Niger. Plusieurs soldats tués, 5 employés blessés, 2 blocs de logements détruits et moyens de traitement endommagés.
- 19/06/2008 : Attaque du champ pétrolifère « Bonga » par des hommes armés dans des vedettes rapides. Plusieurs blessés. Fermeture du champ qui compte pour 10% de la production du Nigéria avec environ 225 000 barils par jour. Impact ressenti sur la montée des prix à l'échelle internationale.
- 31/10/2008 : Attaque du ravitailleur offshore Sagitta de l'armateur français Bourbon par des pirates lourdement armés au Cameroun - 10 personnes kidnappées.
- 07/01/2009 : Attaque d'une plate forme d'Exxon Mobil par des hommes armés dans un navire à fond-plat Vol d'argent et d'objets de valeur.
- 23/01/2009 : Attaque d'un ravitailleur offshore par 10 hommes armés dans 2 vedettes rapides Vol d'argent et d'objets de valeur.
- 26/05/2009 : attaque contre une installation de la compagnie française TOTAL sur le champ pétrolier d'Amenam au Nigéria.

La préservation de l'intégrité des installations pétrolières offshore est un enjeu majeur à l'échelle

mondiale<sup>1</sup>, et amène à s'interroger sur les conséquences qui peuvent découler de la conjonction de la piraterie et du terrorisme, aujourd'hui actifs même en haute mer, pour la sécurité d'approvisionnement énergétique.

Sur le plan international, l'inquiétude des états en terme de protection des installations offshore se retrouve dans des positionnements de plus en plus notables sur la question : que ce soit les Etats-Unis, l'Australie, les Pays Bas, ou la Norvège, tous les pays occidentaux producteurs de pétrole offshore ont pris conscience de la réalité de la menace asymétrique vis-à-vis de la sécurité des plates-formes offshore et mettent en place des mesures visant à renforcer la sécurité maritime offshore.

Il est symptomatique que des scénarios d'attaques organisées commencent à circuler où l'on évoque par exemple l'attaque simultanée de plusieurs plates-formes. Les spécialistes soulignent également le fait que le besoin énergétique va conduire à explorer et exploiter des zones de plus en plus sensibles.

Fournissant déjà plus de 20% de l'approvisionnement mondial, l'activité parapétrolière offshore est en forte croissance à l'inverse de cette même activité en onshore. Les compagnies parapétrolières concentrent à présent la majorité de leurs efforts sur les activités d'exploration et de production offshore qui vont en s'accroissant : à moyen terme plus de la moitié du pétrole et du gaz seront extraits de l'offshore et particulièrement de l'offshore profond (plus de deux cent mètres).

En 2008 il existait environ 3 500 puits forés en mer de par le monde et il s'était construit environ 420 plates-formes offshore, fixes et flottantes. Le marché du forage représentait environ 45 G\$ et celui de l'ingénierie, des équipements et des constructions en mer environ 50 G\$ (source IFP).

Il faut bien reconnaître qu'alors même que ces infrastructures sont conçues pour affronter des environnements naturels extrêmes, elles ne sont pas suffisamment protégées face aux actes de malveillance intentionnels. Les plates-formes offshore forment un réseau industriellement abouti en ce qui concerne l'exploitation mais du point de vue de la sécurité, elles représentent des cibles isolées et exposées à des intrusions à partir de la mer.

Bien évidemment, toutes les plates-formes ne sont pas également exposées. Néanmoins, les brèches existantes dans la protection des infrastructures énergétiques offshore face à la menace terroriste et à la piraterie représentent des points faibles critiques économiquement. Au-delà de cet

aspect purement économique, il est évident que l'effet indirect de la réussite répétée de telles attaques sur la confiance publique internationale serait important.

L'on notera enfin que les intérêts français sont en ce domaine très nombreux : l'industrie parapétrolière française occupe aujourd'hui le quatrième rang mondial dans son secteur d'activité et ce, malgré l'absence de marché national. En 2008, le chiffre d'affaires total de l'industrie parapétrolière française est pour plus de 25% dégagé par l'activité offshore (soit 9 G\$ sur un total de 33 G\$), la France étant dans le domaine leader mondial (source IFP).

## 2.2 Contexte social et réglementaire

Les plates-formes pétrolières sont à l'interface entre le monde maritime et le monde de l'industrie pétrolière. C'est en fait plus l'extrême hétérogénéité des règles applicables que l'absence de droit qui font du statut juridique des plates-formes pétrolières un puzzle compliqué.

Bien que positionnées en mer, les plates-formes pétrolières peuvent avoir un statut tout à fait particulier du fait de leur activité. En dehors des phases d'exploitation, ces infrastructures sont soumises aux risques de la mer et par voie de conséquence aux règles relatives aux événements de mer élaborées par le droit maritime. Avec l'exploitation pétrolière la plate-forme change de cadre et d'univers, et passe du droit international au droit national de l'Etat côtier.

A ce contexte déjà complexe s'ajoutent les règles relatives au droit social applicable au personnel avec des différenciations suivant leur statut.

## 2.3 État de l'art

SARGOS s'inscrit dans le cadre de la protection des infrastructures, et plus spécifiquement de la protection maritime courte à moyenne portée.

A ce jour, nous n'avons pas relevé l'existence de système réellement opérationnel dédié à la protection des plates-formes offshore prenant en charge l'ensemble du processus d'alerte et de réponse graduée vis-à-vis d'intrusions ou de menaces marines.

Cette absence de solution disponible est nettement ressentie au travers de l'offre très générique que l'on trouve dans la littérature ouverte qui reste essentiellement au niveau conceptuel<sup>[1-3]</sup>. Ainsi, la veille faite par le consortium sur ces sujets révèle un traitement indifférencié de la protection des infrastructures critiques avec généralement une même approche pour un aéroport, un port ou une plate-forme offshore. Sachant que quand la spécificité offshore est mise en avant, le problème de base que pose la détection de petites cibles dans le fouillis de mer n'est jamais évoqué.

Les seuls systèmes ayant une finalité pouvant être rapprochée de celle du système SARGOS ont été conçues pour répondre à des besoins militaires d'autodéfense d'un bâtiment ou de défense de zone d'une force navale. Ce sont

<sup>1</sup> A titre d'exemple, on peut rappeler l'impact du cyclone Katrina sur le marché de l'énergie : alors que moins de 5% des plates-formes du golfe du Mexique sont détruites ou sérieusement endommagées, au lendemain de la catastrophe, les tensions sur les marchés pétroliers couplées à l'incertitude sur l'approvisionnement suscitée par l'absence de renseignements, font que le prix du baril enregistre un nouveau record et atteint la barre des 70 \$, le prix du super augmente de 30%... Afin de restaurer la confiance dans le marché pétrolier, l'AIE est contrainte de mener une action collective et les pays membres sont invités à puiser dans leur réserves stratégiques 2 millions de barils par jour pendant 30 jours.

des systèmes d'informatisation de la situation tactique des bâtiments, très spécifiques et excessivement coûteux (plusieurs dizaines de M€), conçus pour être mis en œuvre par une armée de métier bien formée avec du personnel militaire dédié aux tâches de défense sous commandement spécialisé ce qui n'est évidemment pas le cas pour le personnel des plates-formes d'exploitation pétrolières et gazières. De plus, ils n'ont pas été prévus à l'origine pour traiter la menace « asymétrique » Ils ne sont donc pas transposables à la problématique SARGOS.

Ceci étant, dans le domaine de la détection en environnement marin, il existe :

- Des systèmes à base de Radar à impulsions tels que par exemple les Radars de veille ou de navigation de type TERMA, FURUNO, RACAL ou DECCA, ou encore le système Sea-Giraffe d'Ericsson.  
Ces systèmes sont destinés à détecter en priorité des mobiles coopératifs de taille importante ou moyenne. Ils ont des performances jugées insuffisantes face à de petites cibles marines de faible signature radar ou optronique, bien entendu non coopératives (absence de réflecteur radar ou d'AIS), évoluant dans une mer formée (fouillis de mer) et sont pénalisés par une zone aveugle à faible distance du porteur. Par ailleurs, les systèmes à balayage sont généralement relativement lents pour analyser un domaine étendu.
- Des systèmes de surveillance optroniques (développés par exemple par SAGEM, EADS, THALES, RADAMEC, ALENIA, HGH, FLIR Systems, etc.)  
Ces systèmes peuvent être handicapés par les problèmes de réflexion solaire sur la mer et restent sensibles aux conditions météorologiques, leur portée étant rapidement réduite en présence de brume ou brouillard, et d'embruns
- Dans le domaine militaire, des conduites de tir optroniques, systèmes multisenseurs extrêmement onéreux conçus pour diriger avec grande précision des moyens létaux contre des menaces aériennes rapides.

On commence à voir émerger dans le milieu maritime des modules innovants de détection de comportements suspects. Ainsi par exemple, le projet SCANMARIS<sup>[4-8]</sup>, coordonné par DCNS/SIS avec la participation de SOFRESUD, traite la détection de comportements anormaux de manière globale et long terme, en analysant le trafic maritime régulier et en le croisant avec des bases de données sur les navires, pour identifier des suites spatio-temporelles d'anomalies.

Enfin, dans le domaine de la gestion de crise aujourd'hui, le raisonnement / diagnostic est soit humain, soit probabiliste. Les algorithmes que l'on trouve dans la littérature sont généralement construits de façon très linéaire, déterministe ou probabiliste conduisant à des insuffisances dans l'évaluation et la planification de la réaction.

## 3. SARGOS

### 3.1 Présentation

SARGOS vise à concevoir et développer un système global d'alerte et de réponse graduée prenant en compte toute la chaîne de traitement depuis la détection d'une menace potentielle jusqu'à la mise en œuvre de la réaction, en s'intégrant dans les modes de fonctionnement de l'infrastructure et en prenant en compte les contraintes réglementaires et juridiques.

L'aspect novateur réside en premier lieu dans le caractère global de l'approche retenue, et ensuite dans son articulation dans les trois niveaux suivants :

- a) Le niveau d'une détection d'un objet marin de faible dimension dans un périmètre de protection rapproché par mer agitée en utilisant les avancées de la technologie du radar à onde continue couplée à de nouveaux algorithmes de traitement de signal, avec un taux de fausse alarme faible.
- b) Le niveau d'élaboration d'un plan de réaction vis-à-vis de l'intrusion décelée, prenant en compte l'enrichissement progressif de la connaissance et de la nature de l'objet détecté par des attributs de caractérisation de celui-ci. Le processus d'acquisition de la connaissance employé permet le déclenchement au moment approprié de réponses graduées prenant en compte le contexte de la crise (règles de sécurité en vigueur sur la plate-forme, environnement géopolitique, aspects juridiques) ;
- c) Le niveau de gestion de la panoplie des moyens de réaction soit internes à la plate-forme offshore (mise en sécurité), soit externes pour riposter à la menace (injonction, intimidation, activation de moyens non létaux) et diffuser l'alerte vers les autorités locales.

Cette approche système et transverse fait appel à des compétences pluridisciplinaires qui sont capitalisées dans un consortium de partenaires complémentaires regroupant des industriels (SOFRESUD, RCF, DCNS, CS-SI) et des organismes de recherches (ARMINES / CRC, CDMT, TESA, CTSN) travaillant sous le pilotage d'opérateurs majeurs du domaine (TOTAL, GDF-Suez, DGA, Marine Nationale) regroupés dans un comité des utilisateurs.

Bénéficiant du savoir faire des partenaires du groupement, le projet propose d'apporter une solution globale innovante dans le domaine du déclenchement et du traitement d'une alerte dans un périmètre de sécurité prédéfini avec :

- L'analyse du besoin et des vulnérabilités avec le comité des utilisateurs ;
- L'extension des capacités offertes par la technologie radar à onde continue (CW : Continuous Wave) dans les domaines aéronautique et terrestre aux contraintes techniques spécifiques au domaine maritime ;
- Le développement d'algorithmes spécifiques de traitement du signal pour détecter, poursuivre et classer des petites cibles (de faible SER et bien

entendu non coopérantes) à l'approche dans des conditions d'environnement perturbées ;

- Le développement de processus de décision à base d'inférence pour élaborer des plans de réaction réversibles prenant en compte l'enrichissement progressif des critères de caractérisation de l'entité surveillée (comportement cinématique, identification, réaction aux injonctions déclenchées) ;
- La cohérence des plans de réaction ci-dessus avec les impératifs juridiques propres au statut particulier des structures offshore implantées en mer dans diverses zones nationales ou extranationales ;
- L'adaptation au contexte offshore de systèmes de protection maritime, comprenant des moyens préalables d'avertissement puis d'intimidation voire enfin de neutralisation non létale à l'encontre d'embarcations de dangerosité confirmée.

Le schéma fonctionnel du système SARGOS est représenté sur la figure 1. On notera que SARGOS fournit l'alerte à partir d'un cœur de système basé sur la technologie radar à onde continue innovante de RCF mais est apte à prendre en compte les données externes disponibles par ailleurs (pistes du radar de navigation, informations AIS, imagerie thermique, communications externes, etc.) en tant que de besoin pour mettre en place un processus planifié et gradué de réaction.

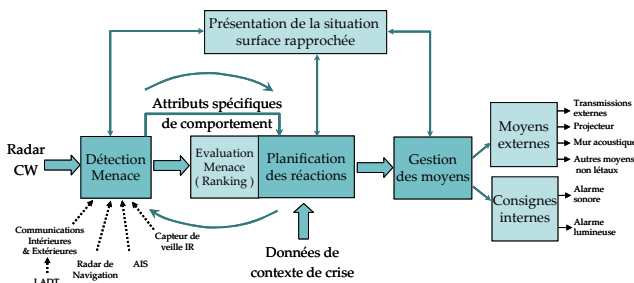


FIG. 1 : Schéma fonctionnel SARGOS

### 3.2 Positionnement

Les problématiques de sûreté maritime sont adressées à ce jour dans des axes complémentaires via différents projets de R & D, expérimentations et systèmes opérationnels :

- Les projets SCANMARIS<sup>[4-8]</sup> et TAMARIS<sup>[9-10]</sup> coordonnés par DCNS (sélectionnés par l'ANR en 2007 et 2008) travaillent sur la génération d'alarmes documentées à partir de la détection de comportements anormaux de manière globale et long terme, en analysant le trafic maritime régulier pour identifier des suites spatio-temporelles d'anomalies. Ils seront prochainement complétés par la plate-forme SISMARIS (FUI) et par le projet d'intégration européen I2C.

- Le projet MWPS<sup>[11-12]</sup> (FUI) coordonné par CS propose un système de protection des environnements portuaires orienté réaction rapide, dans lequel un opérateur prend la décision de mettre en œuvre graduellement des moyens de réaction non létaux.
- Plusieurs expérimentations basées sur des détecteurs optroniques (SAGEM/VIRMA, HGH/VIGISCAN, Sea On Line, FLIR) sont en cours et devraient représenter ultérieurement un complément intéressant pour SARGOS en ce qui concerne l'aide à l'identification.
- Les systèmes civils de type VTS sont largement opérationnels mais d'une part leurs modes de détection usuels sont inappropriés pour ce contexte et d'autre part leur finalité de gestion du trafic maritime est très différente du concept de sécurité global de SARGOS.
- Les systèmes militaires navals classiques sont opérationnels dans leur contexte propre mais ne sont pas transposables en l'état car :
  - Ils n'ont pas été prévus à l'origine pour la « menace asymétrique » ;
  - Le personnel militaire est dédié aux tâches de défense ce qui n'est évidemment pas le cas pour le personnel des plates-formes parapétrolières ;
  - Les coûts seraient prohibitifs dans le cadre industriel car les équipements militaires navals sont développés en très faible série avec des contraintes très élevées.

En complément des projets et systèmes cités ci-dessus, SARGOS s'adresse prioritairement à la protection maritime rapprochée caractérisée par un faible temps de réaction face à des intrusions difficilement détectables par les moyens classiques. SARGOS propose une approche novatrice pour la caractérisation d'une alerte en développant une logique d'analyse du comportement sur le franchissement graduel d'étapes dans un univers temps réel.

A la différence de ces projets et systèmes, SARGOS propose un processus automatisé d'analyse de situation, de levée d'alerte et d'élaboration d'un plan de réponses progressives et réversibles pour la mise en œuvre des moyens de réaction.

Dans le cadre de SARGOS, il est notamment proposé d'étendre les capacités du radar à onde continue de RCF, grâce à la coopération entre RCF, développeur du concept radar et TéSA, laboratoire de renommée internationale dans tous les domaines du traitement du signal, qui développeront les algorithmes spécifiques à la détection et au tracking d'une cible marine de faible dimension par mer formée avec la collaboration de DGA/DET/CTSN.

Il est également proposé d'intégrer des acquis de MWPS dans SARGOS, en les étendant aux systèmes embarqués.

## 4. Approche Scientifique

### 4.1 Détection et classification de la menace

SARGOS propose de lever les insuffisances des systèmes actuels de détection de menace en expérimentant la technologie radar à onde continue dans le domaine marine.

Cette technologie a été retenue car elle apporte une réelle alternative aux technologies « radar pulsé » et « optronique thermique » principalement dans sa capacité à détecter de petites cibles dans des conditions d'environnement particulières.

Si les concepts de base des formes d'ondes continues sont connus depuis de très nombreuses années, leur mise en œuvre a été généralement limitée à des applications courtes distances (inférieure au kilomètre) par des contraintes technologiques liées à :

- la génération de la forme d'onde : problèmes de pureté spectrale et de qualité de la forme d'onde générée ;
- la puissance de traitement bien insuffisante des calculateurs : l'implémentation d'algorithmes de détection et de discrimination distance et vitesse par FFT multiples requiert de grandes capacités de mémoires et de cellules logiques ainsi qu'une grande rapidité de traitements parallélisables.

Les récentes avancées technologiques destinées au secteur des Télécommunications mobiles et digitales ont amené sur le marché de nouveaux composants (Microcontrôleurs, FPGA, Synthèse Numérique Directe, Convertisseurs Analogiques Numériques) à gravure fine qui permettent d'élargir le champ d'applications des radars CW. Ainsi, la technologie innovante radar CW de RCF démontre déjà une efficacité prometteuse dans les domaines aéronautique et terrestre.

Dans le cadre du projet SARGOS, un module radar CW spécifique pour application marine est développé, avec une portée augmentée à environ 8 km, afin d'assurer un délai de préavis suffisant à la prise en charge de la menace tout en gardant le bénéfice de la résolution du radar.

Les capacités SARGOS reposent également sur le développement de modèles, algorithmes et traitements novateurs pour la détection robuste, la poursuite, et la classification de petites cibles marines en environnement perturbé, et en particulier en cas de mer formée se traduisant sur une image radar par la présence d'un fouillis noyant le signal, dû à la combinaison des multiples petits échos parasites renvoyés par la surface agitée de l'eau (« clutter » de mer). Les axes de recherche concerneront plus particulièrement :

- La mise en œuvre de méthodes de filtrage particulière émergentes pour la détection et la poursuite des cibles<sup>[13]</sup> ;
- L'analyse des informations supplémentaires contenues dans l'écho radar pour déterminer des éléments de

signature des menaces considérées (comme le sillage par exemple) ;

- L'exploration des possibilités de modélisation conjointe de la chaîne détection-classification par réseau de neurones.

### 4.2 Formalisation, modélisation et mise en œuvre de la réaction

SARGOS s'adresse prioritairement à la surveillance et la protection d'infrastructures civiles : il ne doit pas requérir de personnel dédié dont le métier serait d'assurer la défense des biens et des personnes et il doit rester compatible d'une exploitation par un opérateur généraliste ayant comme principal objectif la production journalière et qui serait potentiellement stressé par la situation de crise à laquelle il serait confronté.

Il y a aujourd'hui dans la problématique qui nous intéresse un vrai déficit en matière de construction de diagnostic.

Pour lever cette insuffisance, nous proposons une démarche nouvelle d'élaboration automatique de plans de réaction adaptés à la nature de l'intrusion détectée, aux modes de fonctionnement de l'infrastructure et au contexte réglementaire et juridique. Il sera en particulier étudié l'apport dans le contexte du couplage des approches d'inférence bayésienne et de raisonnement à base de cas :

- Le raisonnement à base de cas est mis en œuvre pour combler le manque de connaissance a priori de l'objet considéré et de retour d'expérience dans le domaine applicatif.
- La base de cas est ensuite modélisée par un réseau bayésien, l'approche bayésienne étant privilégiée car elle est particulièrement adaptée aux tenants et aboutissants de la problématique SARGOS, avec notamment :
  - La manipulation simultanée de données capteur mesurées et de connaissance dans une perspective plutôt probabiliste ;
  - La manipulation des incertitudes pour prendre en compte de nouvelles informations avec leur indice de confiance associé ;
  - L'attention centrée exclusivement sur les composants du problème en relation avec la tâche de décision présente.

On notera que si les modèles théoriques et les algorithmes relatifs à l'inférence bayésienne sont connus depuis plusieurs années, les applications opérationnelles relèvent toutefois de processus d'innovation industrielle.

Les capacités de déclenchement d'actions à caractère sécuritaire ou dissuasif visées dans le cadre du projet SARGOS s'appuient :

- Sur les moyens innovants d'avertissement, d'intimidation et de neutralisation issus du système

MWPS (Maritime Warning & Protection System) à l'encontre de menaces potentielles puis avérées ;

- Sur la spécification de procédures d'alerte du personnel, des autorités compétentes et de mise en sécurité de la plate-forme.

Le système MWPS, conçu pour la protection des sites maritimes onshore<sup>[11-12]</sup>, a été retenu car il propose une panoplie de moyens de réactions non létaux innovants et adaptés à la graduation de réponse recherchée dans SARGOS, avec notamment l'injonction à moyenne distance par messages lumineux et sonores puissants et ultra-directifs ou encore la dissuasion par « canon sonore ».

D'autres moyens de réaction non létaux sont actuellement en cours d'analyse, tels que les lanceurs pneumatiques ou les canons hydropropulseurs.

L'objectif scientifique et technique dans le cadre de SARGOS est d'intégrer les acquis du système MWPS compte tenu du contexte et des contraintes inhérentes à une plate-forme offshore :

- Système soumis aux mouvements de roulis / tangage ;
- Planification sélective de la mise en œuvre des moyens de réaction en fonction de la nature de l'intrusion.

### 4.3 Evaluation et validation

Tous les modules de la chaîne de traitement seront implémentés dans une maquette de laboratoire qui permettra d'évaluer le concept et d'illustrer de manière générique le potentiel de la technologie proposée dans SARGOS.

Les activités d'évaluation porteront aussi bien sur le concept que sur le démonstrateur qui est la réalisation physique du concept. Elles seront également déclinées sur les différents niveaux autour desquels s'articule l'approche SARGOS :

- la détection robuste d'un objet flottant ;
- l'élaboration automatique d'un plan de réaction ;
- la gestion de la panoplie des moyens de réaction.

Valider le concept SARGOS, c'est mesurer la sûreté et la rapidité de la décision. Cette validation se fera sur la base de scénarios représentatifs contrastés qui seront définis avec le comité des utilisateurs.

Des campagnes d'essais seront menées notamment sur le site de Saint-Mandrier avec le concours de DGA/DET/CTSN. Elles permettront de valider le concept du projet SARGOS et d'évaluer le gain en sécurité ainsi accessible.

Sur cette base, le comité des utilisateurs comprenant TOTAL, GDF-Suez, DGA/DET, la Marine Nationale et d'autres entités représentatives auront les éléments en main pour valider l'intérêt fonctionnel du projet SARGOS.

## 5. Conclusion

La problématique de la protection des infrastructures civiles critiques vis-à-vis d'intrusions malveillantes nécessite de développer des stratégies assurant de manière coordonnée la chaîne globale de protection consistant en la surveillance automatique, la détection robuste, l'ajustement pertinent du plan d'action en réponse et la mise en œuvre graduée de la réaction.

Le projet SARGOS propose un système global d'alerte et de réponse graduée, pour répondre au fort besoin émergeant de sécurisation des infrastructures offshore civiles, vulnérables aux actes de malveillance, de piraterie ou de terrorisme menées à partir de la mer. Ce système traite :

- La détection automatique robuste et la classification de cibles marines de faibles dimensions par mer formée ;
- La détection de comportements suspects dans un périmètre de sécurité autour de la plate-forme ;
- La formalisation et la modélisation de réactions internes et externes graduées adaptées à la dangerosité de l'intrusion détectée et prenant en compte les règles de sécurité en vigueur sur la plate-forme, l'environnement géopolitique et les aspects juridiques ;
- Le déclenchement d'actions de réaction progressives et réversibles, selon un processus intelligent d'analyse de la situation, et pouvant aller jusqu'à la mise en œuvre de moyens à capacité non létale.

Le consortium est composé d'une PME (SOFRESUD), d'industriels (DCNS, RCF, CS-SI), et de laboratoires de recherche (ARMINES/CRC, TésA, CDMT) avec le soutien d'organismes publics (DGA/DET/CTSN).

Les travaux seront effectués sous l'égide d'un comité de pilotage comprenant des représentants des deux principales sociétés pétrolières et gazières françaises TOTAL et GDF SUEZ, de la DGA et de la Marine Nationale, réunis dans un comité des utilisateurs qui sera sollicité pour communiquer l'expression de besoin, consolider les objectifs techniques, valider les scénarios de travail et évaluer la pertinence des résultats obtenus.

Le projet SARGOS comporte des expérimentations par mer formée qui bénéficieront de la mise à disposition du centre naval de Saint-Mandrier.

## Remerciements

Le projet SARGOS a été sélectionné par l'Agence Nationale de la Recherche (ANR) pour être subventionné dans le cadre du programme 2010 sur les concepts systèmes et outils pour la sécurité globale (CSOSG).

Le projet SARGOS d'une durée de 30 mois a démarré en janvier 2010 pour se conclure en juillet 2012.



## Références

- [1] Honeywell. *Maritime Security: Meeting Threats to the Offshore oil and Gas Industry* □May 2008
- [2] Thales Group *Security Solutions for the oil and Gas Industry*
- [3] *Securing Oil & Gas Assets* Society of Petroleum Engineers, 20-22 oct. 2008
- [4] P. Georgé, JP. Mano, MP. Gleizes, M. Morel, A. Bonnot, D. Carreras. *Emergent Maritime Multi-Sensor Surveillance Using an Adaptive Multi-Agent System (regular paper)* Cognitive systems with Interactive Sensors (COGIS 2009), Paris, 16/11/2009-18/11/2009, SEE/URISCA, (support électronique), novembre 2009
- [5] F. Jangal, JP. Georgé, A. Bonnot, MA. Giraud, M. Morel, A. Napoli. *Toward a complete system for surveillance of the whole EEZ: SCANMARIS and associated projects*. Oceans'09, Biloxi, Mississippi, USA, 26/10/2009-29/10/2009
- [6] A. Littaye, MA. Giraud, JP. Mano, A. Bonnot, A. Napoli, M. Botalla, F. Jangal, M. Morel. *SCANMARIS : détection des comportements anormaux des navires* Workshop Interdisciplinaire sur la Sécurité Globale (WISG09), Troyes, 27/01/2009-29/01/2009
- [7] M. Morel, A. Napoli, A. Littaye, MP. Gleizes, P. Glize. *ScanMaris: an Adaptive and Integrative Approach for Wide Maritime Zone Surveillance*. Cognitive systems with Interactive Sensors (COGIS 2007), Stanford University California USA, 26/11/2007-27/11/2007, p. 1014, 2007
- [8] A. Littaye, M. Morel, A. Bonnot, A. Napoli, JP. Georgé, MA. Giraud, F. Jangal, M. Botalla. *Trafic Maritime : détection des comportements anormaux é des navires*. Journées scientifiques et techniques du CETMEF □Paris □8, 9 et 10 décembre 2008
- [9] M. Morel, A. Littaye, C. Saurel, O. Poirel, A. Napoli, S. Valle, G. Proutière-Maulion. *TAMARIS, Traitement et Authentification des MenAces et RISques en mer ;* Workshop Interdisciplinaire sur la Sécurité Globale (WISG09), Troyes, 27/01/2009-29/01/2009.
- [10] M. Morel, C. Saurel, O. Poirel, P. Salom, A. Napoli. *TAMARIS*. MAST 2009, Stockholm, Suède
- [11] D. Chaumartin, J. Déon, C. Granet, M. Grimaldi, Y. Lacroix, G. Tedeschi. *Maritime Warning and Protection System* Actes colloque WISG'09 (Janv. 2009).
- [12] D. Chaumartin *Maritime Warning and Protection System*. Journées scientifiques et techniques du CETMEF □Paris □8, 9 et 10 décembre 2008.
- [13] C. Andrieu, M. Davy, A. Doucet. *Efficient Particle Filtering for Jump Markov Systems. Application to Time-Varying Autoregressions*, IEEE Trans. On Signal Processing, Vol. 51, No. 7, pp 1762-1770, July 2003.